Information Technology Control Framework in the Federal Government – Considerations for an Audit Strategy

Presentation to The Institute of Internal Auditors Breakfast Session

February 6, 2014
Outline of Presentation

- Overview of Shared Services Canada (SSC)
- Information Technology (IT) Controls – Theory and Practice
- Considerations for an Audit Strategy of an IT Control Framework
Fragmentation in the management of the Government’s IT infrastructure has led to high costs, complexity and security risks

Mission-critical programs depend on IT infrastructure • 2,100 mission-critical programs that span: • Key benefits programs (e.g. employment insurance, Canada Pension Plan, Old Age Security); • Security (e.g. Department of National Defence, Royal Canadian Mounted Police’s Canadian Police Information Centre systems and provincial police force databases, Canada Border Services Agency border systems, and Public Safety cyber security and emergency response); • Safety and health (e.g. Canadian Food Inspection Agency [CFIA] and food monitoring, Health Canada labs, Environment Canada weather systems, Natural Resources Canada seismic systems); • Farmers and students (Agriculture and Agri-Food Canada, CFIA, loan programs); and • Finance systems (e.g. Canada Revenue Agency federal-provincial tax and benefit systems, Financial Transactions and Reports Analysis Centre of Canada ).

Departments managed their IT infrastructure independently • In total, the Government of Canada (GC) was spending $1.9B/year on an unstructured and uncoordinated web of IT infrastructure and services: • 63 email systems; • Nearly 500 data centres of varying sizes, quality, security and energy efficiency; and • 50 wide area networks connecting over 3 500 buildings and data centres – over 1 000 firewalls.

Status quo was complex, costly and less secure • Current state of IT infrastructure is: • Vulnerable to cyber attacks, low availability and poor performance; • A long-term unfunded liability and a barrier to renewal, modernization and agility; • Using procurement practices that limit innovation; • Largely in-sourced; and • Not service-oriented.
Current State of Data Centres and Networks

- **485 data centres**
- **50 wide area networks (WAN)**
- **4 000+ local area networks (LAN)**

**Department A:** small data centre

**Department B:** small data centre

**Department H:** small data centre

**Department Q:** small data centre

**Department F:** small data centre

**Building**

- **LAN1** – Dept. A
- **LAN2** – Dept. B
- **LAN3** – Dept. F
- **LAN4** – Dept. H
- **LAN5** – Dept. Q

**Building**

- **LAN6**
- **LAN7**

**Building**

- **Dept. F: small data centre**
- **LAN6**
- **LAN7**

**Building**

- **Dept. D: small data centre**
- **LAN6**
- **LAN7**
Shared Services Canada (SSC) was established to address these problems through an enterprise-wide approach to IT service and renewal

- In 2011, the Prime Minister created SSC to:
  - improve IT service delivery across the GC;
  - transform the GC’s email, data centres and networks; and
  - generate savings for deficit reduction and the longer term.

- Personnel, financial resources and assets were transferred through Orders-in-Council (OiCs) to SSC from 43 of the largest federal departments.

- **SSC in 2013-14**: 5,895 employees; net expenditures of $1.4B (plus $369M in revenues); new responsibility for workplace technology services
Consolidation of personnel, services, assets and contracts has already improved service and value-for-money

• SSC’s initial contribution to deficit reduction was outlined in Economic Action Plan (EAP) 2012:
  ▪ $74.7 million in 2012-2013 (5% of SSC’s base);
  ▪ $104.5 million in 2013-2014 (7% of SSC’s base); and
  ▪ $150 million on an ongoing basis beginning in 2014-2015 (10% of SSC’s base).

• SSC is generating these immediate savings by:
  ▪ building the leanest internal services organization in the GC;
  ▪ leveraging GC buying power to secure better prices from telecommunications and data centre services suppliers; and
  ▪ migrating outdated desktop telephone services to modern and less costly cellular and Voice over Internet Protocol services.

• In addition to generating savings, SSC’s enterprise-wide approach to service delivery is focussed on:
  ▪ enterprise incident management to keep mission-critical systems up and running and address the root causes of any breakdowns;
  ▪ moving from 9-to-5 IT operations teams to 24/7 for mission-critical systems; and
  ▪ contributing to important government-wide priorities (e.g. Beyond the Border, pay and pension modernization).
SSC has developed detailed plans to transform the Government of Canada’s IT infrastructure and is moving to implementation.

**Current State**

- 63 different email systems and no standard for addresses
- 485 data centre sites that are inefficient and vulnerable
- 50 wide area networks and outdated telecommunications services

**Target End State**

- Single email system with a standard naming convention
- Seven data centres that are resilient, secure and energy-efficient
- Single enterprise network and Workplace 2.0 technology

**Lower costs, increased security, improved service**
End State of Data Centres and Networks

**Enterprise Security**

- **Geographic Diversity**
  - Data centres in pairs for high performance and availability
  - Data centres in diverse locations for disaster tolerance

- **Production X**

- **Production Y**

- **Development**
  - Separate development data centres for best support of application development
  - Leading practice to ensure strong segregation of production environment from non-production

**Business Continuity**

**Sensitive Data Enclaves**

**GC Network**

- Regional and International Carriers (377,000 users; 4,000+ sites)

**Virtual Private Cloud**

**Allies (+International)**

**GC Offices**

**Public Servants**

**Canadians**

**Businesses**

**Governments**

**GC Network**

**Internet**

**Regional and International Carriers** (377,000 users; 4,000+ sites)
## Responsibility for IT services across the Government

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Email, Data Centres and Networks</th>
<th>Workplace Technology Devices</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Management and Delivery</td>
<td>SSC</td>
<td></td>
<td>Departments</td>
</tr>
<tr>
<td></td>
<td>(mandatory or optional for specific departments as specified in orders in council)</td>
<td></td>
<td>Public Works and Government Services Canada</td>
</tr>
<tr>
<td>Procurement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy and Standard Setting</td>
<td></td>
<td>Treasury Board of Canada Secretariat</td>
<td></td>
</tr>
</tbody>
</table>
Why do IT Controls Matter?

• Why should I understand IT risks and controls? *Two words: assurance and reliability*
• What is to be protected? *Trust should be protected because it ensures business and efficiency.*
• Where are IT controls applied? *Everywhere.*
• Who is responsible? *Everyone. But controls’ ownership must be defined.*
• When should IT risks and controls be assessed? *Always.*
• How much control is enough? *Management must decide based on risk appetite, tolerance and mandatory regulations.*
Principles for IT Controls @ SSC

- Risk-Based
- Use of Established Control Frameworks
- Validated through consultations (e.g. partners, OAG, OCG)
- Focus on End-State
- Comprehensive (Security, Finance, Operations)
- Designed to provide assurance to partners as well as management
Levels of Controls

- **Entity Level Controls** – are pervasive across a department, and include value and ethics, governance, human resource management, risk management, communication, and monitoring.

- **Business Process Controls** – are controls, both manual and automated, embedded in specific business processes.

- **Information Technology (IT) General Controls** (also referred to as General Computer Controls) – include controls over computer operations, access to programs and data, program development, and program changes.
Figure 3. Understanding the IT environment in a business context.

Figure adapted and revised from: IT Control Objectives for Sarbanes-Oxley, 2nd Ed., used by permission of the IT Governance Institute (ITGI). ©2006 ITGI. All rights reserved.
IT Audit Universe in the Federal Government

SSC Corporate Audits
- e.g.: IT Governance, IT Procurement

Partner’s Audits of IM
- e.g.: Application Controls, Database Mgmt

IT General Controls
- Operational
- Financial
- Security

Legacy MAPs

Assurance to Partners

Joint Audits and Assessments

OAG Audits
Hierarchy of IT Controls

- COSO
- COBIT
- TBS – Policy on Internal Controls
- Canadian Institute of Chartered Accountants (5925)
- Consensus Audit Guidelines (20 critical controls) (SSC–RMF)
- CSEC (ITSG33)
Components of the COSO Framework

• **Control environment** – senior management establishes the tone from the top regarding the importance of internal control and expected standards of conduct, including:
  - Integrity and ethical values – articulated in the Values and Ethics Code for the Public Sector;
  - Organizational structures and assignment of authority and responsibility – articulated, in part, in the Policy on Management, Resources and Results Structures; and
  - Process for attracting, developing and retaining competent individuals.

• **Risk assessment** – a dynamic and iterative process for identifying and analyzing risks to achieving the entity's objectives, forming a basis for determining how risks should be managed:
Components of the COSO Framework (Continued)

- **Control activities** – contributes to the mitigation of risks to the achievements of objectives to acceptable levels:
  - Control activities are manifested in policies that establish what is expected and in relevant procedures to effect the policies; and
  - Control activities are performed at all levels of the entity and at various stages within business processes, and over the technology environment.

- **Information and communication** – enables personnel to understand the entity’s objectives and the importance of their internal control responsibilities.

- **Monitoring activities** – ongoing evaluations are used to ascertain whether controls are present and functioning:
  - Existing mechanisms include the annual Management Accountability Framework (MAF) assessment, the annual Departmental Performance Report, and the risk-based multi-year audit plan updated annually.
Control Environment

• IT is often mistakenly regarded as a separate organization of the business and thus a separate control environment.
• IT is complex, not only with regard to its technical components but also in how those components integrate into the organization’s overall system of internal control.
• IT can introduce additional or increased risks that require new or enhanced control activities to mitigate successfully.
• IT requires specialized skills that may be in short supply.
• IT may require reliance on third parties where significant processes or IT components are outsourced.
• Ownership of IT controls may be unclear, especially for application controls.
## Cross-reference of COSO and CobiT

<table>
<thead>
<tr>
<th>COSO Components</th>
<th>CobiT Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate, Direct and Monitor</td>
<td>Build, Acquire and Implement</td>
</tr>
<tr>
<td>Align, Plan and Organise</td>
<td>Deliver, Service and Support</td>
</tr>
<tr>
<td>Build, Acquire and Implement</td>
<td>Monitor, Evaluate and Assess</td>
</tr>
</tbody>
</table>

### Control Environment

- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring
Interrelationships of CobiT Components

Source: Cobit 4.1, Figure 4 – Interrelationships of CobiT Components
Example: IT Control Objectives for Sarbanes-Oxley

<table>
<thead>
<tr>
<th>IT Control Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Acquire and maintain application software</td>
</tr>
<tr>
<td>2. Acquire and maintain technology infrastructure</td>
</tr>
<tr>
<td>3. Enable operations</td>
</tr>
<tr>
<td>4. Install and accredit solutions and changes</td>
</tr>
<tr>
<td>5. Manage changes</td>
</tr>
<tr>
<td>6. Define and manage service levels</td>
</tr>
<tr>
<td>7. Manage third-party services</td>
</tr>
<tr>
<td>8. Ensure system security</td>
</tr>
<tr>
<td>9. Manage the configuration</td>
</tr>
<tr>
<td>10. Manage problems and incidents</td>
</tr>
<tr>
<td>11. Manage data</td>
</tr>
<tr>
<td>12. Manage the physical environment and operations</td>
</tr>
</tbody>
</table>
Example: CCA – Critical Controls for Effective Cyber Defense

- **Critical Control 1**: Inventory of Authorized and Unauthorized Devices
- **Critical Control 2**: Inventory of Authorized and Unauthorized Software
- **Critical Control 3**: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- **Critical Control 4**: Continuous Vulnerability Assessment and Remediation
- **Critical Control 5**: Malware Defenses
- **Critical Control 6**: Application Software Security
- **Critical Control 7**: Wireless Device Control
- **Critical Control 8**: Data Recovery Capability
- **Critical Control 9**: Security Skills Assessment and Appropriate Training to Fill Gaps
- **Critical Control 10**: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- **Critical Control 11**: Limitation and Control of Network Ports, Protocols, and Services
- **Critical Control 12**: Controlled Use of Administrative Privileges
- **Critical Control 13**: Boundary Defense
- **Critical Control 14**: Maintenance, Monitoring, and Analysis of Audit Logs
- **Critical Control 15**: Controlled Access Based on the Need to Know
- **Critical Control 16**: Account Monitoring and Control
- **Critical Control 17**: Data Loss Prevention
- **Critical Control 18**: Incident Response and Management
- **Critical Control 19**: Secure Network Engineering
- **Critical Control 20**: Penetration Tests and Red Team Exercises

**Source**: Consortium for Cybersecurity Action, *Consensus Audit Guidelines*
Example: CSEC ITSG-33 Security Control Catalogue Structure

<table>
<thead>
<tr>
<th>Classes</th>
<th>Technical Security Controls</th>
<th>Operational Security Controls</th>
<th>Management Security Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AC - Access Control</td>
<td>AT - Awareness &amp; Training</td>
<td>CA - Security Assessment &amp; Authorization</td>
</tr>
<tr>
<td></td>
<td>AU - Audit &amp; Accountability</td>
<td>CM - Configuration Management</td>
<td>PL - Planning</td>
</tr>
<tr>
<td></td>
<td>IA - Identification &amp; Authentication</td>
<td>CP - Contingency Planning</td>
<td>RA - Risk Assessment</td>
</tr>
<tr>
<td></td>
<td>SC - System &amp; Communications Protection</td>
<td>IR - Incident Response</td>
<td>SA - System &amp; Services Acquisition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MA - Maintenance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MP - Media Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PE - Physical &amp; Environmental Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PS - Personnel Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SI - System &amp; Information Integrity</td>
<td></td>
</tr>
</tbody>
</table>

*Source: CSEC, IT Security Risk Management: A Lifecycle Approach.*
Senior Roles and Responsibilities

• **Deputy heads** have always had the responsibility to ensure that internal controls are regularly reviewed in the context of risk, ensuring that those internal controls are balanced against and proportional to the risks they mitigate.

• **Chief Financial Officer** supports the deputy head by establishing and maintaining a system of internal control related to financial management, including financial reporting and departmental accounts.

• **Other senior departmental managers** establish and maintain a system of internal control for their areas of responsibility and within the departmental system of internal control.

• **Chief audit executives** establish risk-based audit plans and perform assurance engagements necessary to provide the deputy head with independent assurance regarding risk management, control and governance processes.

• **Departmental audit committees** are responsible to review and provide advice on the departmental internal control arrangements, and to be informed on all matters of significance arising from work performed by others who provide assurances to senior management and the deputy head.

*Source: Policy on Internal Control; Directive on Internal Auditing in the Government of Canada*
IT Controls Implementation Road Map

1. Plan and scope IT controls
2. Assess IT Risk
3. Document Controls
4. Evaluate Control Design and Operating Effectiveness
5. Prioritize and Remediate Deficiencies
6. Build Sustainability
IT Controls and the Audit Function

• **Generic Description of Internal Controls:**
  - Internal control is a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
    - Effectiveness and efficiency of operations.
    - Reliability of reporting.
    - Compliance with applicable laws and regulations.

  **Source:** COSO

• **Role of audit:**
  - The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization’s governance, operations and information systems.

  **Source:** IIA Standard 2130
Proposed Audit Process of Audit of SSC’s IT Internal Controls

Management Description of SSC’s IT Systems

Management Assertion that description of SSC’s IT systems is fairly presented, controls are suitably designed and operate effectively

Internal Audit Report on SSC’s IT Internal Controls

Departmental Audit and Evaluation Committee (DAEC) provides advice

Office of the Auditor General Provides an Opinion on IT Controls Could Use the Work of SSC Internal Audit Function

SSC Partners
Audit team develops an understanding of overall risks to internal controls

Focus on significant entity-level controls

Focus on specifics controls presenting reasonable possibility of failure

Select these controls for testing
Management of Audits of IT Controls

Planning
- Take stock of Business and IT Processes
- Risk Assessment
- Ensure IT competencies and skills are available

Executing
- Identify and document relevant controls
- Test the design and operating effectiveness of the controls
- Conclude on the controls

Reporting
- Clearly communicate observations and conclusions
- Present to DAEC and External Auditors
- Provide Assurance to Partners
Questions